Station de porte de villa (portier) (VTO2111DPS2)

Guide de démarrage rapide

V1.0.0

Avant-propos

Général

Ce manuel présente la structure et la configuration de base de la station de porte (VTO ou portier).

Précautions d'emploi

Les mentions d'avertissement catégorisées suivantes ayant une signification définie apparaîtront dans le manuel.

Mentions d'avertissement	Signification
 **AVERTISSEMENT**	Indique une situation moyennement ou faiblement dangereuse qui entraînera des blessures faibles ou modérées si les instructions données ne sont pas respectées.
 **AVERTISSEMENT**	Indique une situation potentiellement dangereuse qui pourra entraîner des dommages de la propriété, des pertes de données, une performance moindre ou des résultats imprévisibles, si les instructions données ne sont pas respectées.
REMARQUE	Fournit des informations supplémentaires pour mettre en évidence et compléter le texte.

Historique des révisions

Version	Description de la révision	Date de sortie
V1.0.0	Date de sortie	Mars 2020

À propos du manuel

- Le manuel est donné uniquement à titre de référence. Si des incohérences existent entre le manuel et le produit réel, vous devrez tenir compte du produit réel.
- Nous ne serons pas tenus responsables pour toute perte causée par une utilisation non conforme aux instructions contenues dans ce manuel.
- Le manuel pourra être actualisé selon la réglementation et les lois les plus récentes des régions concernées. Pour des informations détaillées, reportez-vous au manuel au format papier, sur CD-ROM, disponible en numérisant le code QR ou sur notre site Web officiel. Si des incohérences existent entre le manuel au format papier et le manuel au format électronique, vous devrez tenir compte de la version électronique.
- Tous les logiciels et toutes les interfaces présentés ici sont susceptibles d'être modifiés sans préavis écrit. Les mises à jour du produit peuvent apporter des différences entre le produit réel et le manuel. Veuillez contacter le service client pour être informé des dernières procédures et obtenir de la documentation supplémentaire.

- De légères variations ou des erreurs d’impression peuvent apparaître au niveau des caractéristiques techniques, des fonctions et de la description des opérations. En cas d’incertitude ou de désaccord, veuillez vous référer à notre dernière explication.
- Mettez à jour le logiciel de lecture ou essayez un autre logiciel de lecture grand public si le manuel (au format PDF) ne s’ouvre pas.
- Les marques de commerce, les marques déposées et les noms des sociétés dans ce manuel sont de la propriété respective de leurs propriétaires.
- Veuillez visiter notre site Web, contacter le fournisseur ou le service après-vente si un problème survient pendant l’utilisation de l’appareil.
- En cas d’incertitude ou de désaccord, veuillez vous référer à notre dernière explication.

Précautions et avertissements importants

La description ci-dessous constitue la méthode d'utilisation appropriée de cet appareil. Veuillez lire attentivement le manuel avant de l'utiliser afin d'éviter tout danger et toute perte matérielle. Veuillez vous conformer strictement aux instructions contenues dans ce manuel pendant l'utilisation de l'appareil et conserver correctement le document après lecture.

Conditions de fonctionnement

- Évitez de placer ou d'installer l'appareil dans un lieu exposé directement aux rayons du soleil ou à proximité des appareils de chauffage.
- Évitez d'installer l'appareil dans une zone humide, poussiéreuse ou fuligineuse.
- Placez l'appareil à l'horizontale ou installez-le sur une surface stable pour éviter toute chute.
- N'éclaboussez pas et ne faites pas couler de liquide sur l'appareil ; ne posez rien sur l'appareil qui contienne du liquide afin d'éviter que celui-ci ne pénètre dans l'appareil.
- Installez l'appareil dans un endroit bien ventilé et n'obstruez pas ses orifices de ventilation.
- N'utilisez l'appareil que dans la plage d'entrée et de sortie nominale.
- Évitez de démonter l'appareil au hasard.
- Transportez, utilisez et conservez l'appareil dans la plage d'humidité et de température autorisée.

Alimentation électrique

- Le produit doit utiliser les fils électriques (fils d'alimentation) requis par la région où l'appareil sera utilisé.
- Veuillez utiliser une source d'alimentation satisfaisant aux exigences d'extrabasse tension de sécurité (SELV) et dont la tension nominale est conforme aux exigences de source d'alimentation limitée prescrites par la norme IEC60950-1. Pour connaître les exigences spécifiques en matière d'alimentation électrique, reportez-vous aux étiquettes de l'appareil.
- Le coupleur d'appareil est un dispositif de déconnexion. Lors d'une utilisation normale, gardez un angle qui facilite le fonctionnement.

Table des matières

1 Introduction

Après déballage, assurez-vous que la station de porte de villa n'est pas endommagée et que tous les accessoires sont présents (notamment la station de villa, le guide de démarrage rapide et le kit de vis).

Figure 1-1 Illustration

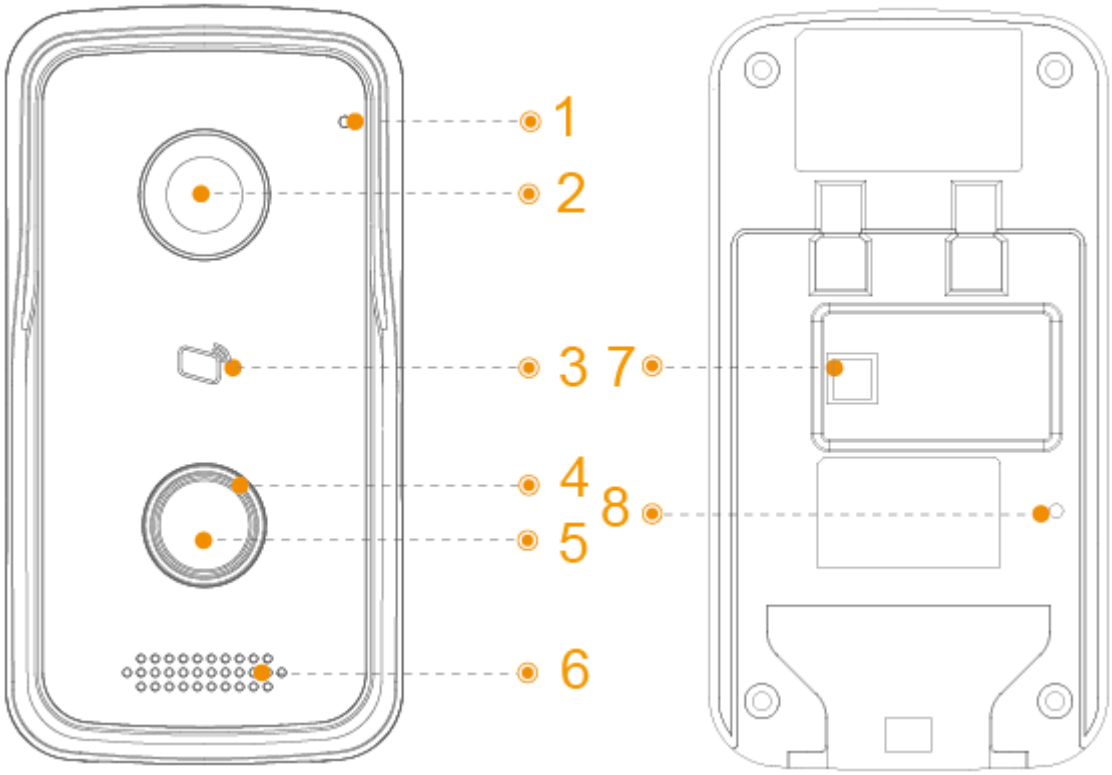

Tableau 1-1 Description de port

N°	Nom	N°	Nom
1	MICROPHONE	5	Bouton d’appel
2	Caméra	6	Haut-parleur
3	Lecteur de carte d’accès	7	Contact antisabotage
4	Voyant d’état	8	Réinitialiser

2 Installation de l’application et ajout d’appareils

Scannez le code QR suivant pour télécharger et installer l’application.

Figure 2-1

Avant d’ajouter la station de porte (VTO) à gDMSS Plus, vous devez modifier l’adresse IP de la station de porte (VTO), vous assurer que la station de porte (VTO) et le routeur sont connectés au même réseau, et connecter la station de porte (VTO) à la source d’alimentation.

Sur votre téléphone portable, appuyez sur , puis suivez les instructions à l’écran jusqu’à ce que l’interface de sélection de la région s’affiche.

Sélectionnez une région.

Appuyez sur Terminé dans le coin supérieur droit de l’interface.

L’interface En direct s’affichera.

En direct

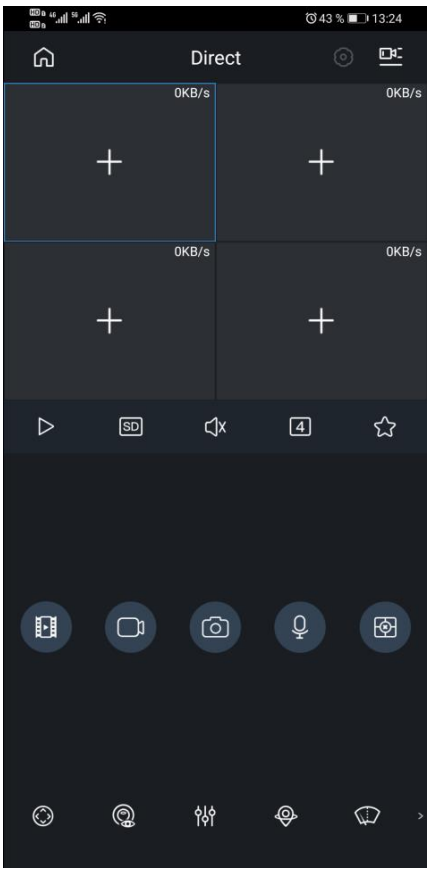

Figure 2-2

Appuyez sur dans le coin supérieur gauche de l’interface En direct.

L’interface Habitation s’affichera.

Habitation

Figure 2-3

Appuyez sur depuis l’interface Habitation.

L’interface Gestionnaire des appareils s’affichera.

Appuyez sur dans le coin supérieur droit de l’interface Gestionnaire des appareils

Gestionnaire des appareils

Figure 2-4

Appuyez sur l’adresse IP/le domaine.

L’interface Ajouter un appareil s’affiche.

Ajout d’un appareil

Figure 2-5

Appuyez sur VTO depuis l’interface Ajouter un appareil.

L’interface Ajouter un appareil s’affiche.

Ajout d’un appareil

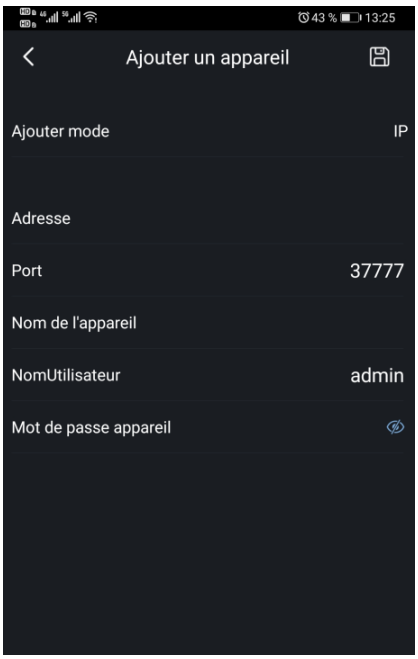

Figure 2-6

Remplissez les champs Address (adresse IP de la station de porte (VTO)), Device Name (Nom de l’appareil) et Device Password (Mot de passe de l’appareil).

Appuyez sur .

La station de porte (VTO) est ajoutée. Vous pouvez regarder les vidéos capturées par la station de porte (VTO), appeler la station de porte (VTO), déverrouiller les portes lorsqu’il y a un appel de la station de porte (VTO), et plus encore.

Porte

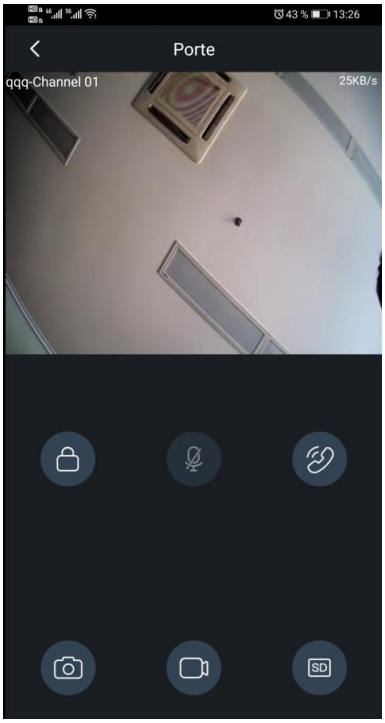

Figure 2-7

Appendix 1 FAQ

1. **Le dispositif ne fonctionne pas normalement.**
   Réinitialisez le dispositif et reconfigurez les paramètres.
2. **Comment réinitialiser le dispositif ?**
   Appuyez et maintenez le bouton de réinitialiser enfoncé pendant 10 secondes.
3. **Le dispositif est hors ligne.**
   Si le voyant ne cesse de clignoter en bleu, le dispositif est hors ligne. Vérifiez la connexion réseau. Si la connexion réseau est normale, réinitialisez le dispositif et reconfigurez les paramètres.

Appendix 2 Recommandations en matière de cybersécurité

La cybersécurité est plus qu'un mot à la mode : c'est quelque chose qui concerne chaque appareil connecté à Internet. La vidéosurveillance sur IP n'est pas à l'abri des cyberrisques, mais la mise en place de mesures élémentaires pour protéger et renforcer les réseaux et les appareils en réseau les rendra moins vulnérables à des attaques. Nous donnons, ci-après, des conseils et des recommandations pour créer un système de sécurité plus sûr.

Actions obligatoires à prendre pour la sécurité réseau d'équipements de base :

1. **Utiliser des mots de passe robustes**

   Veuillez vous référer aux recommandations suivantes pour définir les mots de passe :

   - La longueur du mot de passe doit être d'au moins 8 caractères ;
   - Ils doivent être composés de deux types de caractères comprenant des lettres majuscules et minuscules, des chiffres et des symboles ;
   - Ils ne doivent pas être composés du nom du compte dans l'ordre normal ou inversé ;
   - Les caractères ne doivent pas se suivre, par ex. 123, abc, etc. ;
   - Les caractères ne doivent pas se répéter, par ex. 111, aaa, etc. ;

2. **Mettre à jour le micrologiciel et le logiciel client à temps**

   - Conformément à la procédure standard de l'industrie technologique, nous vous recommandons de maintenir à jour le micrologiciel de votre équipement (enregistreurs NVR et DVR, caméra IP, etc.) afin de garantir que votre système est doté des correctifs de sécurité les plus récents. Lorsque l'équipement est connecté au réseau public, il est recommandé d'activer la fonction de vérification automatique de la disponibilité de mises à jour afin d'obtenir rapidement les informations sur les mises à jour du micrologiciel fournies par le fabricant.
   - Nous vous conseillons de télécharger et d'utiliser la version du logiciel client la plus récente.

Recommandations à suivre pour améliorer la sécurité réseau de votre équipement :

1. **Protection matérielle**

   Nous vous suggérons de fournir une protection matérielle à vos équipements, en particulier les dispositifs de stockage. Par exemple, placez l'équipement dans une armoire ou une salle informatique spéciale, et appliquez des autorisations de contrôle d'accès et une gestion des clés sur mesure afin d'empêcher à tout personnel non autorisé d'entrer en contact physique avec les équipements pour éviter par ex. d'endommager le matériel, des connexions non autorisées à des équipements amovibles (disque flash USB, port série) etc.

2. **Modifier régulièrement votre mot de passe**

   Nous vous conseillons de modifier régulièrement vos mots de passe pour réduire les risques qu'ils soient devinés ou déchiffrés.

3. **Définir et mettre à jour les informations de réinitialisation des mots de passe à temps**

   L'équipement prend en charge la fonction de réinitialisation du mot de passe. Veuillez définir les informations relatives à la réinitialisation du mot de passe à temps, y compris l'adresse électronique de l'utilisateur final et les questions de protection du mot de passe.

Si les informations changent, veuillez les modifier à temps. Lors de la configuration des questions de protection du mot de passe, il est conseillé de ne pas utiliser des questions (réponses) trop faciles à deviner.

4. **Activer le blocage de compte**

   La fonction de blocage de compte est activée par défaut. Nous vous recommandons de la laisser activée pour garantir la sécurité des comptes. Si un pirate tente de se connecter plusieurs fois avec un mot de passe incorrect, le compte concerné et l'adresse IP de la source seront bloqués.

5. **Modifier les ports par défaut des services HTTP et d'autres services**

   Nous vous conseillons de modifier les ports par défaut du service HTTP et des autres services en les choisissant dans la plage numérique allant de 1 024 à 65 535, ce qui permet de réduire le risque que des étrangers puissent deviner les ports utilisés.

6. **Activer HTTPS**

   Nous vous conseillons d'activer le protocole HTTPS. Vous accéderez ainsi au service Web au moyen d'un canal de communication sécurisé.

7. **Activer la liste blanche**

   Nous vous conseillons d'activer la fonction de liste blanche pour empêcher tout le monde, à l'exception des adresses IP spécifiées, d'accéder au système. Par conséquent, veillez à ajouter l'adresse IP de votre ordinateur et l'adresse de l'équipement qui l'accompagne à la liste blanche.

8. **Liaison d'adresse MAC**

   Nous vous recommandons de lier l'adresse IP et l'adresse MAC de la passerelle à l'équipement, réduisant ainsi le risque d'usurpation ARP.

9. **Assigner raisonnablement les comptes et les privilèges**

   En fonction des besoins d'activité et de gestion, ajoutez de manière raisonnable des utilisateurs et leur assigner un ensemble d'autorisations minimales.

10. **Désactiver les services inutiles et choisir les modes sécurisés**

    S'ils ne sont pas nécessaires et pour réduire les risques, désactivez certains services, tels que SNMP, SMTP, UPnP, etc.

    En cas de besoin, il est fortement recommandé d'utiliser les modes sécurisés, y compris mais sans limitation, les services suivants :

    - SNMP : choisissez SNMP v3 et configurez des mots de passe de chiffrement et d'authentification robustes.
    - SMTP : choisissez le protocole TLS pour accéder aux serveurs de messagerie.
    - FTP : choisissez le protocole SFTP et définissez des mots de passe robustes.
    - Point d'accès : choisissez le mode de chiffrement WPA2-PSK et définissez des mots de passe robustes.

11. **Chiffrement de la transmission audio et vidéo**

    Si vos contenus de données audio et vidéo sont très importants ou sensibles, nous vous recommandons d'utiliser la fonction de chiffrement de la transmission, afin de réduire les risques de vol des données audio et vidéo durant la transmission.

    Rappel : le chiffrement de la transmission entraînera une certaine baisse de l'efficacité de la transmission.

12. **Contrôle sécurisé**

    - Vérifier les utilisateurs connectés : nous vous conseillons de vérifier régulièrement les utilisateurs connectés afin de savoir si la connexion à l'appareil s'effectue sans autorisation.

- Consulter le journal de l'équipement : en examinant les journaux, vous pouvez connaître les adresses IP utilisées pour la connexion à vos appareils et les principales opérations effectuées.

13. Journal réseau

Comme la capacité de stockage de l'équipement est limitée, le journal stocké sera limité. Si vous devez conserver le journal pour longtemps, il est recommandé d'activer la fonction de journal réseau afin de veiller à ce que les journaux essentiels soient synchronisés avec le serveur de journal réseau pour suivi.

14. Construire un environnement réseau sécurisé

Afin de garantir au mieux la sécurité des équipements et de réduire les cyberrisques potentiels, nous vous recommandons de :

- Désactiver la fonction de mappage de ports du routeur pour éviter les accès directs aux appareils Intranet à partir du réseau externe.
- Compartimenter et isoler le réseau en fonction des besoins réseau réels. Si la communication n'est pas nécessaire entre deux sous-réseaux, il est conseillé d'utiliser les technologies de réseau VLAN, GAP et d'autres pour compartimenter le réseau de sorte à obtenir une isolation réseau effective.
- Mettre en place le système d'authentification d'accès 802.1x pour réduire le risque d'accès non autorisés aux réseaux privés.
- Il est recommandé d'activer le pare-feu de votre routeur ou les fonctionnalités de liste blanche et de liste noire pour réduire le risque d'attaque informatique.